(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 April 2004 (01.04.2004)

PCT

(10) International Publication Number
WO 2004/028077 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number:
PCT/EP2003/007829

(22) International Filing Date: 18 July 2003 (18.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
02020583.7 17 September 2002 (17.09.2002) EP

(71) Applicant and
(72) Inventor: PITSOS, Errikos [DE/DE]; Florian-Geyer-Str. 10, 81377 München (DE).

(74) Agent: GRÜNECKER, KINKELDEY, STOCKMAIR & SCHWANHÄUSSER; Maximilianstrasse 58, 80538 München (DE).

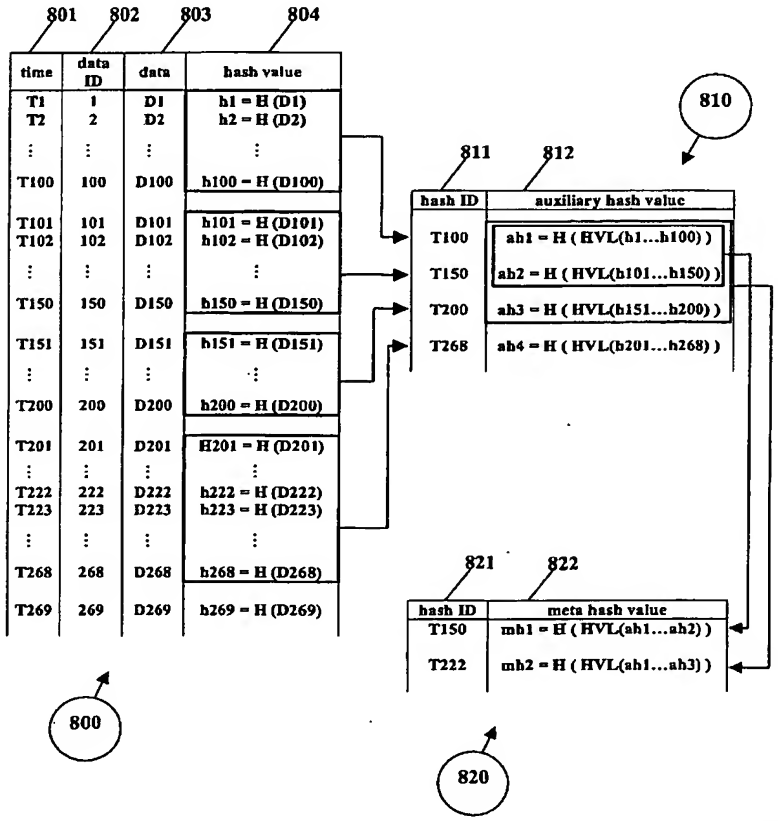
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: METHODS AND SYSTEMS FOR PROVIDING A SECURE DATA DISTRIBUTION VIA PUBLIC NETWORKS



(57) Abstract: A server in a public key system stores a list of fingerprints of digital data. Another fingerprint is computed for this list of fingerprints and provided to a client terminal. A client terminal in a public key system obtains a list of fingerprints of digital data from a first source in this system. The client terminal further obtains a fingerprint for that list of fingerprints from a first source as well as from a second source for comparing both obtained fingerprints.

WO 2004/028077 A1

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Int[redacted] Application No
PCT/[redacted] 03/07829

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	EP 0 940 945 A (AT & T CORP) 8 September 1999 (1999-09-08) column 1, line 12 - line 22 ---	1,2,23, 24
X A	US 6 304 974 B1 (SAMAR VIPIN) 16 October 2001 (2001-10-16) abstract column 4, line 34 - line 38 column 5, line 63 -column 7, line 37 figures 1-4 ---	1,2,12 13
A	US 2002/073310 A1 (IBM CORPORATION) 13 June 2002 (2002-06-13) abstract paragraph '0051! - paragraph '0053!; figure 4 --- -/--	1,2

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
9 February 2004	23. 02. 2004

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Dujardin, C

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Int[redacted] Application No
PCT/[redacted]03/07829

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 530 757 A (KRAWCZYK HUGO M) 25 June 1996 (1996-06-25) abstract figures 3-5	1,2
A	US 2001/032310 A1 (CORELLA FRANCISCO) 18 October 2001 (2001-10-18) page 5, paragraph 64 - paragraph 76; figures 1-3 page 8, paragraph 113 - paragraph 114; figure 12 page 14, paragraph 204 - paragraph 205; figure 20	1,2
A	US 6 144 739 A (WITT DON EARL ET AL) 7 November 2000 (2000-11-07) column 3, line 43 -column 4, line 48; figure 1	9,10
A	US 2002/112163 A1 (IRETON MARK) 15 August 2002 (2002-08-15) abstract figure 2	1,2
A	US 5 050 212 A (DYSON PATRICK) 17 September 1991 (1991-09-17) column 2, line 57 -column 4, line 29; figure 2	1,2
X	US 6 240 187 B1 (LEWIS TONY) 29 May 2001 (2001-05-29) abstract column 3, line 9 -column 4, line 48 column 5, line 13 -column 8, line 60 figures 1-7	41-72
X Y A	US 2002/126849 A1 (HESS PENNINGTON J ET AL) 12 September 2002 (2002-09-12) abstract paragraph '0017! - paragraph '0026! paragraph '0049! - paragraph '0059! paragraph '0159! - paragraph '0165!	41-72 112,113 116,117
X	EP 0 898 260 A (NTT DATA CORP ;NIPPON TELEGRAPH & TELEPHONE (JP)) 24 February 1999 (1999-02-24) abstract paragraph '0021! - paragraph '0031! paragraph '0033! - paragraph '0063! figures 1-6	58-72

-/--

INTERNATIONAL SEARCH REPORT

Int[redacted] Application No
PCT/[redacted]03/07829

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	US 2001/055395 A1 (VOGLER DEAN H) 27 December 2001 (2001-12-27) abstract paragraph '0011! - paragraph '0020! figures 1-4	41-44
A	WO 01 06702 A (POSTE ;FRANCE TELECOM (FR); REMERY PATRICK (FR); TRAORE JACQUES (F) 25 January 2001 (2001-01-25) abstract page 3, line 17 -page 19, last line	73-104
A	GRAY A: "ROUTER ENCRYPTION MADE EASY - THE HARD WAY" DATA COMMUNICATIONS, MCGRAW HILL. NEW YORK, US, vol. 26, no. 2, 1 February 1997 (1997-02-01), page 36,38 XP000659573 ISSN: 0363-6399 page 36, right-hand column, line 11 - line 35	83
X	DE 198 22 795 A (SIEMENS AG) 25 November 1999 (1999-11-25)	105-110, 115,119, 120,124, 125
Y	abstract	112,113
A	column 5, line 61 -column 7, line 23; figures 1A-1B	121,126, 127,130, 135-139

INTERNATIONAL SEARCH REPORT

application No.
PCT/EP 03/07829

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. ☒ As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☐ No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

☐ The additional search fees were accompanied by the applicant's protest.

☒ No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-40

   Computing/obtaining the fingerprint of a list of fingerprints of digitally encoded data in a public key system

2. Claims: 41-72

   Preventing cryptographic operations (encryption, decryption or signature) in a public key system by preventing the use of the private or of the public key of a first key pair and replacing the first key pair by a second key pair for executing the cryptographic operations.

3. Claims: 73-104

   Layered asymmetric encryption of digital data or layered digital signature of hashed digital data in a data distribution system

4. Claims: 105-139

   Using the hash value of a random token and of a fixed random value as a key for symmetric encryption/decryption

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/[redacted]03/07829

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0940945	A	08-09-1999	EP	0940945 A2	08-09-1999
			JP	11338780 A	10-12-1999
US 6304974	B1	16-10-2001	NONE		
US 2002073310	A1	13-06-2002	NONE		
US 5530757	A	25-06-1996	JP	8016104 A	19-01-1996
US 2001032310	A1	18-10-2001	AU	2792801 A	24-07-2001
			EP	1250774 A2	23-10-2002
			JP	2003534677 T	18-11-2003
			WO	0152470 A2	19-07-2001
US 6144739	A	07-11-2000	NONE		
US 2002112163	A1	15-08-2002	GB	2374172 A	09-10-2002
			JP	2002358011 A	13-12-2002
US 5050212	A	17-09-1991	NONE		
US 6240187	B1	29-05-2001	US	5761306 A	02-06-1998
			AU	723946 B2	07-09-2000
			AU	2137797 A	10-09-1997
			GB	2324449 A ,B	21-10-1998
			WO	9731450 A1	28-08-1997
US 2002126849	A1	12-09-2002	US	6212280 B1	03-04-2001
			AU	1448800 A	15-05-2000
			AU	2020300 A	15-05-2000
			CA	2347176 A1	04-05-2000
			CA	2347211 A1	04-05-2000
			EP	1131912 A1	12-09-2001
			EP	1121780 A1	08-08-2001
			JP	2002529008 T	03-09-2002
			JP	2002529012 T	03-09-2002
			WO	0025473 A1	04-05-2000
			WO	0025466 A1	04-05-2000
			US	6442690 B1	27-08-2002
			US	2001026619 A1	04-10-2001
EP 0898260	A	24-02-1999	EP	0898260 A1	24-02-1999
			US	6377692 B1	23-04-2002
			JP	10260630 A	29-09-1998
			WO	9832113 A1	23-07-1998
US 2001055395	A1	27-12-2001	NONE		
WO 0106702	A	25-01-2001	FR	2796788 A1	26-01-2001
			AU	6577900 A	05-02-2001
			EP	1195020 A1	10-04-2002
			WO	0106702 A1	25-01-2001
			JP	2003505927 T	12-02-2003
DE 19822795	A	25-11-1999	DE	19822795 A1	25-11-1999
			WO	9960747 A2	25-11-1999
			EP	1080557 A2	07-03-2001
			JP	2002516521 T	04-06-2002